City of Douglas
Administrative Policies

4.04 Internet / Email Usage and Security

Effective August 10, 2000 *(formerly Policy 2000-2)*
Revised: November 23, 2004

Purpose:

To define appropriate use of the City of Douglas's network, computers, all related peripherals, software, electronic communications and/or Internet access. These policies apply to the access of the City's network, use of computing technology resources, and use of the City's Internet access at any location, from any device, and via wired or wireless communication. They apply to all users of City technology resources, regardless of employment status.

Policy:

A) Authorized and Appropriate Uses

The City authorizes its staff, contractors, volunteers and others to carry out legitimate City business through use of the City's computing and network resources, including Internet access. All users of City computing and network resources must do so in an ethical, legal and responsible manner. All such use must be consistent with all pertinent City policies and work rules, as well as the following:

1. Online Forums: City employees may participate in online forums, including but not limited to newsgroups or chats, in the course of business when relevant to their duties, under the following conditions:

    a. Each user of the City's Internet facilities shall identify himself or herself honestly, accurately and completely (including one's City affiliation and function where requested) when participating in online forums or setting up accounts on outside computer systems.

    b. Employees must keep in mind that they are at all times representing the City, and any comments must be reflective of City policy unless expressly indicated otherwise.

c. Users must refrain from any unauthorized political advocacy or unauthorized endorsement or appearance of endorsement by the City of any commercial product or service.

2. News Briefing Services: In the interest of keeping the City well-informed, City employees may subscribe to news briefing services pertinent to each employee's position with the City, such as MSNBC.

3. E-mail: Users should consider e-mail communications to be equivalent to any other form of written communication. Just like other forms of communication, e-mail communications may be public records, are subject to the same record retention policies and procedures, and may be copied and/or forwarded to other users without your knowledge or consent. Users should use the same care in drafting and editing e-mail communications as with any other form of written communication.

4. Personal Use: Employees may use the City's network and computer resources, including Internet access, for non-business research or browsing during mealtime or other breaks, or outside of work hours, or as approved by a supervisor, provided such use complies with any and all pertinent City policies and does not result in additional cost or liability; interfere with City business, productivity or performance; or pose additional risk to security, reliability or privacy. Employees should conduct only non-private activities, as they have no right to privacy when using the City's resources. See Section C, below.

5. Passwords: User IDs and passwords help maintain individual accountability for network, computer and Internet resource usage. Employees are required to maintain strict confidentiality of any and all passwords. Such passwords are the property of the City and must be provided to the City upon termination of employment, whether voluntary or involuntary, and at any time upon request by authorized MIS Department staff.

6. Viruses: Any file that is downloaded onto the City's network or computing systems must be scanned for viruses before being run or accessed.

7. Off-Peak Use: Certain network, Internet or other computer uses create significant data traffic, cause network congestion and must be scheduled for off-peak times. Examples of such uses include video and audio streaming and downloading, large file transfers, mass e-mailings and any other use involving the transmittal of large files. For information on what constitutes an "off-peak time" or whether a particular use should be scheduled for an off-peak time, you should contact the City's MIS Department.

8. Connections: Users must obtain approval from the MIS Department before connecting any devices to the City's network, including but not limited to PCs, laptops, PDAs, hubs, printers, scanners, remote connections and wireless or wired devices. In order to protect the security of the City's network and computing resources, any computer used for independent dial-up Internet access or leased-line connections to any outside computer or network must be physically isolated from the City's internal networks. Any exceptions to this rule must be approved by the City's MIS Department. For information on whether a particular use falls within this provision, you should contact the City's MIS Department.

9. Encryption: Confidential email documents and respective attachments sent over the Internet may require use of Encryption Technologies. Encryption routines will be determined by the MIS Department staff.

B) Prohibited Uses

The following uses of the City's network and computing resources, including Internet access, are strictly prohibited and may result in disciplinary action up to and including termination. Any employee, contractor, or volunteer engaging in a prohibited use may be denied future use of any or all of the City's computing systems (Exceptions to this section may be authorized by the City Manager as part of security testing and limited strictly to MIS Department staff.)

1. The display of any kind of sexually-explicit image or document on any City system is a violation of the City's policy on sexual harassment. In addition, sexually-explicit material may not be archived, stored, distributed, edited or recorded using the City's network or computing resources.

2. The City uses independently supplied software and data to identify inappropriate or sexually-explicit Internet sites. We may block access from within the City's networks to any such sites. If you find yourself connected accidentally to a site that contains sexually-explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program, and report the incident to your supervisor.

3. The City prohibits the use of its network and computing resources, including Internet access, in any illegal or unethical manner, including:

    a. Downloading or distributing pirated software, audio files or other data or any other misappropriation or theft of intellectual property;

    b. Deliberately propagating any virus, worm, Trojan horse, or backdoor program code or any other use that may cause damage to the system or breach the confidentiality of any other user;

c. Knowingly disabling or overloading any computer system or network or circumventing any system intended to protect the privacy or security of another user;

d. Releasing non-public City information publicly via any newsgroup, chat or other computerized means, whether intentional or inadvertent;

e. Sending mass unsolicited e-mailings for any reason other than legitimate City business (i.e., "spam");

f. Misusing City assets or resources;

g. Attempting to disable, defeat or circumvent any City security facilities, including firewalls, proxies, Internet address screening programs and other security systems;

h. Any use that may compromise the security and/or integrity of the City's network and computing resources or any confidential information;

i. Any use that violates City policies and/or procedures;

j. Any use that harms or brings discredit to the City.

4. Users may download executable software from the City's FTP server. However, executable software from outside sources, including the Internet may only be downloaded with the express approval of the City's MIS Department. Downloaded software must be used only under the terms of its license.

5. Users may not upload onto the Internet, and may not share in any other manner, any software licensed to the City, or data owned or licensed by the City, without explicit authorization from the MIS Department.

6. Users of the City's network are strictly prohibited from establishing Internet servers such as FTP, WWW, Gopher, Telnet, E-mail or any other type of Internet server on a City computer.

7. The City's network and computing resources may not be used to facilitate the operation of personal businesses, such as sale of cosmetics or consulting.

C) No Right of Privacy

The City owns all data stored on its network and systems, including e-mail, Internet usage logs, and other stored files or documents. Users have no right of privacy in any use of the City's network and computing resources, including Internet access. The City

reserves the right to inspect any and all files stored in any areas of its network and computing resources, whether public or private, in order to assure compliance with City policies.

Any software or files downloaded, whether via the Internet or otherwise, into the City network or computers become the property of the City. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. In addition, the City retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.

The City reserves the right to monitor, record, review, transmit and/or archive any and all City network and computer resource usage, including Internet access, at any time, for any reason, and without notice to any user. The City may conduct random and requested audits of employee accounts in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the City, to assist Departments in evaluating performance issues and concerns, and to identify productivity or related issues. Only employees authorized by the City Manager may conduct the monitoring and auditing activities described in this paragraph, and such activities must be limited to the parameters of such authorization.

The City of Douglas will comply with lawful requests from government, law enforcement and regulatory agencies, including courts, for any information regarding or stored in the City's network and/or computing resources.

Unauthorized use of Internet, e-mail or any City technology; or unauthorized monitoring/auditing of City systems may result in discipline up to and including termination.

Approved by: _____.

Acting City Manager Date